

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-96043

(43)公開日 平成8年(1996)4月12日

(51)Int.Cl.⁶

識別記号

庁内整理番号

FI

技術表示箇所

G 0 6 F 17/60

19/00

H 0 4 Q 7/38

G 0 6 F 15/ 21

3 4 0 B

15/ 30

C

審査請求 未請求 請求項の数19 FD (全 10 頁) 最終頁に続く

(21)出願番号 特願平7-264673

(22)出願日 平成7年(1995)9月20日

(31)優先権主張番号 3,104,41

(32)優先日 1994年9月22日

(33)優先権主張国 米国 (US)

(71)出願人 390035493

エイ・ティ・アンド・ティ・コーポレーション

AT&T CORP.

アメリカ合衆国 10013-2412 ニューヨーク
ニューヨーク アヴェニュー オブ
ジ アメリカズ 32

(72)発明者 ビー. ワーリング パトリッジ

アメリカ合衆国, 07931 ニュージャージー
一, ファー ヒルズ, オーランド ロード
900

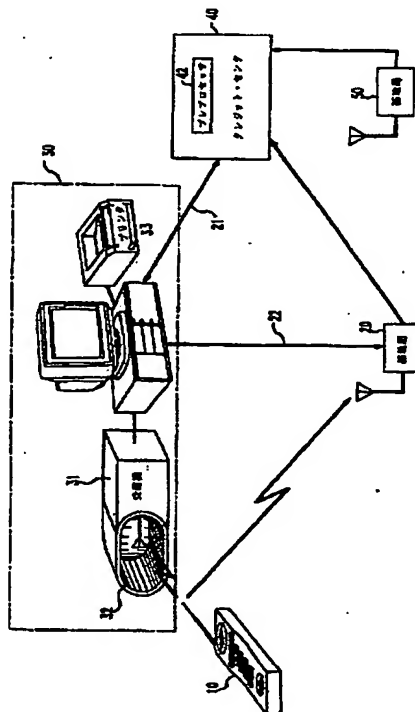
(74)代理人 弁理士 三俣 弘文

(54)【発明の名称】 アクション保証方法とクレジット提供配置

(57)【要約】

【課題】 認証されたトランザクション・コントローラのセル式電話を介し例えば、顧客にクレジットを提供する配置を提供する。

【解決手段】 本発明の実施の形態として、例えば、業者から商品またはサービスの購入にクレジットを求める顧客がそのセル式電話を起動し、このセル式電話をそのセル式電話サービス提供者の基地局に対して認証し、クレジットを得るよう結合の設定に進む。この被呼側電話番号に対応する通常の番号シーケンスとは異なる特有のシーケンスをセル式電話サービス提供者に送信してクレジットを得る。このシーケンスには業者のIDコードと所望クレジット金額を含む。



1

【特許請求の範囲】

【請求項 1】 (A) 通信用に設けた無線通信装置 (10) を起動する起動ステップと、

(B) この無線通信装置が発信する信号に基づきこの無線通信装置の識別を認証する認証ステップと、

(C) この無線通信装置によって許可された特定のアクションを実行するアクション実行ステップとを有することを特徴とするユーザのためのアクションを保証するアクション保証方法。

【請求項 2】 前記 (B) 認証ステップは、前記無線通信装置を通信利用に使用する場合に前記無線通信装置が使用する登録プロトコルの少なくとも一部に少なくとも部分的に対応するプロトコルを使用することを特徴とする請求項 1 に記載の方法。

【請求項 3】 前記 (B) 認証ステップは、前記無線通信装置を通信利用に使用する場合に前記無線通信装置が使用する登録プロトコルに少なくとも部分的に対応するプロトコルを使用することを特徴とする請求項 1 に記載の方法。

【請求項 4】 前記ユーザのための前記アクションは、前記ユーザにクレジットを供与するクレジット供与ステップであることを特徴とする請求項 1 に記載の方法。

【請求項 5】 前記クレジット供与ステップは、通信サービスを前記無線通信装置に提供する通信サービス提供者によって行われることを特徴とする請求項 4 に記載の方法。

【請求項 6】 前記クレジット供与ステップは、通信サービスを前記無線通信装置に提供する通信サービス提供者以外の通信サービス非提供者によって行われることを特徴とする請求項 4 に記載の方法。

【請求項 7】 前記ユーザのための前記アクションは、特定の行先へ保証制御信号を送信する保証制御信号送信ステップであることを特徴とする請求項 1 に記載の方法。

【請求項 8】 前記ユーザのための前記アクションは、行先へ制御信号を送信する制御信号送信ステップであることを特徴とする請求項 1 に記載の方法。

【請求項 9】 前記行先はホーム・コントローラ基地局 (50) であることを特徴とする請求項 8 に記載の方法。

【請求項 10】 前記行先は、テレビジョン・セットへ信号を提供する信号提供者と対話するホーム・コントローラ基地局 (60) であることを特徴とする請求項 8 に記載の方法。

【請求項 11】 前記クレジット供与ステップは、トランザクション・パスワード部分列、クレジット金額部分列、ID 部分列および検証部分列を含む列データをクレジット提供センタに送信するステップを有することを特徴とする請求項 4 に記載の方法。

【請求項 12】 無線電話を持ちおよびクレジット提供

2

センタ (40) と関係を持つ第 1 の当事者に第 2 の当事者の利益のためにクレジットを提供するクレジット提供配置において、

(A) 無線通信用に前記無線電話が使用する識別プロトコルと適合する識別プロトコルを使用し前記クレジット・センタに対し前記無線電話を識別する第 1 の手段と、

(B) 前記第 2 の当事者の識別とクレジット合計金額を前記第 1 の手段によって識別された無線電話と関係付ける第 2 の手段と、

(C) 前記クレジット・センタが前記第 2 の当事者に承認ステータスを通信する第 3 の手段を有することを特徴とするクレジット提供配置。

【請求項 13】 前記第 1 の手段と前記第 2 の手段と前記第 3 の手段の基本的要素は前記クレジット提供センタの制御下にあることを特徴とする請求項 12 に記載の配置。

【請求項 14】 前記第 1 の手段はセルラ電話基地局とこのセルラ電話基地局と前記クレジット・センタ間の通信リンクを有することを特徴とする請求項 12 に記載の配置。

【請求項 15】 前記第 1 の手段は前記クレジット・センタと通信するため前記第 2 の当事者の構内に送信装置 (30) を持つことを特徴とする請求項 12 に記載の配置。

【請求項 16】 前記第 2 の当事者の構内の前記送信装置はセルラ電話基地局を介し前記クレジット・センタと通信することを特徴とする請求項 15 に記載の配置。

【請求項 17】 前記第 1 の手段と前記第 2 の手段と前記第 3 の手段の基本的要素は前記第 2 の当事者の構内に配置することを特徴とする配置。

【請求項 18】 前記第 1 の手段はさらに前記無線電話と通信するため受信装置 (31) を有することを特徴とする請求項 17 に記載の配置。

【請求項 19】 さらに、前記無線電話からの送信を他の無線電話からの送信から判別する手段を有することを特徴とする請求項 18 に記載の配置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、無線電話に係り、特にこの無線電話の保持者のためのアクションを保証する無線電話の利用プロセスに関する。

【0002】

【従来の技術】 現在無線電話は専ら通信用に利用されている。一方ユーザのためのアクションを保証するためには次例のような別の装置が利用されている。例えば、赤外線方式の遠隔制御装置を利用して TV や VCR などを制御する。また家のキーを利用して家の中へ入ることを保証する。またクレジット・カードを利用して顧客クレジットを得る例などである。これらの活動をすべて“制御トランザクション”と分類することができる、という

のはこのユーザによって制御が行われある所望の結果または利益が得られるからである。

【0003】これらトランザクションの中であるものは無料であって、例えば、自分の家に入ることを保証する例、TVの無料チャネルの受信を制御する例、などを挙げることができる。またあるトランザクションは有料であって、例えば、劇場に入ることを保証する例、視聴当たりの“ペイ”TVチャネルを選択する例、顧客クレジットを得る例、などを挙げることができる。本発明の目的は下記の制御トランザクションに関する課題を解決するシステムを提供することであって次の通りである。

【0004】

【発明が解決しようとする課題】ユーザにその無線電話を利用させ制御トランザクションを行わせるシステムおよび有料の制御トランザクションの場合にはこの制御トランザクションのコストをその無線電話サービス提供者または別の当事者に対しこの無線電話の保持者が持つクレジット口座に負わせるシステムの提供が望まれている。

【0005】

【課題を解決するための手段】本発明は、無線電話を利用してユーザのためのアクションを保証しそれによって保証されたトランザクション・コントローラを形成する。この手順はこの無線電話を起動するとそれに係る認証プロトコルに基くものである。いったんこの無線電話が認証されてしまうと、制御コマンドがその無線電話によって（またはその無線電話によって有効に）発せられ、また必要に応じこの無線電話サービス提供者に対しクレジット合計金額をこの無線電話の保持者が持つクレジット口座に負わせることを許可しそれに債務とする。

【0006】顧客クレジットの受入れを求める利用の場合、例えば、商品やサービスの販売業者（以下単に業者と略す）からそれを購入するためクレジットを求める顧客は次のように行う。この顧客は、その無線電話を起動し、そのローカル基地局を通じてこの無線電話サービス提供者に対しこの無線電話を認証し、クレジットを得るため“対話”を確立するよう進む。クレジットは、特有のシーケンスつまりその被呼側電話番号に対応する通常番号シーケンスと異なるシーケンスとすることができるような特有のシーケンスを無線電話サービス提供者に送信して得られる。このシーケンスに含むものには、業者IDコード（その販売業者を識別するもの）があり、さらに当然のことであるが、所望クレジット金額があり、さらにまた他の情報、例えば、購入アイテムや受けるサービスなどの情報を挙げることができる。

【0007】本発明の実施の別の形態では、この業者の無線受信装置がその基地局へ送信される情報を傍受し、この業者と所望クレジット金額に関する情報を追加し、この情報をそのクレジット提供組織、すなわちこの無線

電話保持者の口座を有する組織、へ送信する。このクレジット提供組織との通信は無線通信または有線通信を通じて行うことができる。このクレジットに対する要求が適切と判断されると、この業者にメッセージを送信し、クレジットの供与を許可し、このトランザクションは成功裡に終了する。この制御トランザクションがその無線電話保持者のクレジット・ラインをアクセスする必要がないような利用の場合、また認証のみが重要であるような場合、例えば、無線電話を利用してそのホーム・ガレージ・ドアを開錠するような場合、無線電話基地局のランダム信号を結合し認証可能な信号を送信することができ、認証されると、その制御トランザクションを行う。

【0008】

【発明の実施の形態】本発明の実施の形態を次の順序で例示し説明する。まず認証と金額交換が非常に重要となる顧客クレジットの供与と取得のプロセスの説明から開始する。次に認証が不可欠であるホームにアクセスするプロセスを説明する。最後にコマンドと制御の機能だけが重要である例えば、TVのような機器を制御するプロセスを説明する。以下の説明はセルラ電話とセルラ電話に利用されるプロトコルを取上げ行う。ただしここで理解する必要があるのは本発明は、他の無線電話に対比すると、例えば、セルラ電話の利用の場合よりさらに広いものである。

【0009】1. クレジット供与

現在では顧客クレジットを供与するプロセスはかなりありふれた動作である。例えば、銀行のような組織が顧客にクレジットを提供し、この顧客にクレジット・カードを供与し、この顧客はこのクレジット・カードを使って商品やビスを購入する。商品やサービスを購入すると、この顧客のカードに対し課金され、代金請求サイクルの最終期限にこの組織がこの顧客に明細書を送付し、支払い期日中にこの顧客はその組織にそれが供与したクレジットの相殺をする。当然のことであるが、クレジット・カードの取得を所望する者はこのクレジットを供与する組織を見付ける必要がある。ところでクレジットを供与する組織を見付けることは多数の人々にとって特に難しい障害ではないが、次の点が注目される。

【0010】それはクレジットの顧客はすでに複数の通信事業体（市内交換局サービス、長距離通信事業体、セル通信事業体）と貸借関係をすでに持っている者が多いということが注目される。ここで一般顧客クレジットを供与するのにこの普及している関係を利用することができないかその可否を問う問題が生ずる。セルラ電話を携帯している人々が多数になってきているのでこの関係を利用しクレジット・カードで一緒に処理できれば確かに好都合である。この機能を以下に説明する配置とプロセスが提供する。図1にセルラ電話10を示すがこれは基地局20と無線通信するため用いられる。基地局20はクレジット・センタ40と通信し、またクレジット・セ

5

ンタ40は業者の機器30と通信する。また基地局50もクレジット・センタ40と通信する。

【0011】クレジット・センタ40と基地局20、50を動作させるセルラ電話サービス提供者が同一組織のものである場合があるが、それに限る必要はない。クレジット・センタ40はこのセルラ電話サービスをそのユーザに提供する組織の中の料金請求取扱部門であるのが通常である。例えば次の場合を仮定する。基地局20はセルラ電話サービス提供者Aに属し、基地局50はセルラ電話サービス提供者Bに属し、およびセルラ電話10の正しい保持者はセルラ電話サービス提供者Bと契約関係を持つ。さらにクレジット・センタ40はセルラ電話サービス提供者Bの料金請求取扱機構とする。またチャンネル21は機器30をクレジット・センタ40に結合するチャンネルであって有線または無線の通信路である。

【0012】安全保証の認証を得ることができると、機器30とクレジット・センタ40間の通信のためいずれか通常のプロトコルを用いることができる。顧客クレジットを取得する場合に関する基本的トランザクションは、セルラ電話10に対しその口座にクレジット・センタ40で選択した金額を課金し、この無線電話保持者の口座に対するこの課金から業者は受益を得ていることをこの業者に通知する。ただしこれはセルラ電話10が正しい顧客の手にあるという前提においてである。簡略のため、このセルラ電話の所持者の正当性に疑問がある場合にそれが係るプロトコルについてはここでは述べない。これには、例えば、顧客のパーソナル識別コードや音声認証などの利用の場合を挙げることができる。

【0013】しかしここで認識することは、これら課題の中の一つにこの供与クレジットの利益をその顧客と業者の両者が受ける保証をするということがある。別の課題はこの顧客もその業者も不利益を得ないよう安全が保証された方法でこのインタラクションを提供することである。さらに別の課題はこの通信によって第三者が不利益を得ないようまた利益を得ようこのインタラクションを提供することである。これらの目的は、ここに引例とする下記特許例を参照とする、ここでは図2に示すが、そのプロトコルによって実現される。それは、米国特許第5、204、902号、Reedsら、1993年4月20日発行、を参照のこと。このReedsらの特許を簡単に述べる。ここでは各セルラ電話には下記のものがある。

【0014】すなわち、各セルラ電話の持つものには、“共用秘密データ”(SSD)のデジタル列データがあつてこれは秘密キー(A-KEY)のハッシュ処理の結合から導かれたものであり、さらにそのセルラ電話装置番号(ESN)があり、またそのセルラ電話割当番号(MIN1)があり、さらにランダム列データがあつてこれはこのセルラ電話ユーザがビジネス関係を持つ組織が選択するものである。代表例として、この組織はセル

6

ラ電話サービス提供者であつてこのセルラ電話サービス提供者とこの顧客が“署名”し、つまり生じた課金を支払う契約関係を持つものである。セルラ電話サービス提供者はその地域が特定の地理的エリアに通常限定される。

【0015】このエリアはその顧客の“ホーム”セルラ電話サービス地理的エリア(ホームCGSA)である。説明の都合上、セルラ電話10のホームCGSAは基地局50であるとする。セルラ電話10が存在するセルの基地局20は“訪問先”ホストCGSAであるとする。このSSD列は2個の列のSSDA列とSSDB列に分けられる。このSSDA列は認証用に用い、SSDB列は通信暗号用に用いる。次に動作で説明する。セル通信網の各セルは(基地局20、50)のような基地局によってサービスされる。この基地局はある選択した繰返しレートでランダム・シーケンス(RAND)を同報通信するが、セキュリティ増強のため比較的頻度多く(例えば、大部分のセル呼出の継続時間よりもっと度々)このRANDを変更する。

【0016】あるセル内にいるセルラ電話に電源を入れると、このRANDシーケンスを受信しそしてそのセルに自分自身を知らせて応答する(セルラ電話10は基地局20が送信するRANDを受信する)。これは登録プロセスであつて図2のライン(プロセス)11、12、13で示される。プロセス11、12、13をさらに具体的に説明する。このセルラ電話はそのESN列とMIN1列をそのSSDA列とRAND列とに連結し、得られた列データをハッシュ処理してそのAUTHR列を得る。次にこのセルラ電話はそのAUTHR列をRAND列とESN列とMIN1列とともにその基地局へ確認のため送信する。

【0017】ここで説明はそれるが、このRAND信号を送信する理由は、セルラ電話10がRANDを受信した時とその基地局がAUTHRを受信する時との間にその基地局がそのRANDを変更したことがあるからであり、ただしこれはオプションであつてというのはその基地局はその最後のRAND列を容易に記憶することができるからである。この基地局はこのESN列とMIN1列を検出してここからそのセルラ電話のアサートされた識別とそのホームCGSAの識別を決定する。説明はそれるが、このホームCGSAを識別するためにはアルゴリズムをこのESN列とMIN1列に適用する必要があるかまたはデータベースに照会する必要がある。

【0018】基地局20はこのホームCGSA、ただしこれは図1の例では基地局50であるが、これからこのSSD列を受信しこのSSDA列をそのRAND列とESN列とMIN1列と結合し得られた列データをハッシュ処理してそのバージョンのAUTHR列を得る。次にこの基地局はそのバージョンのAUTHR列をその受信バージョンのAUTHR列と比較する。これら2個の列

データが一致すると、そのセルラ電話は正しいものと決定される。“OK”信号(ライン13)がこの基地局からそのセルラ電話に送信されこれにはさらに通信するためにこのセルラ電話が使用する必要がある特定の周波数に関する情報を含む。

【0019】この取扱基地局によって登録されると、このセルラ電話は呼出を開始することができるがこれは少なくともあるその被呼電話番号をその他の列データに連結するプロセスで行われる。すなわち、このセルラ電話は、その被呼側の情報であるMIN3列を、そのRAND列とESN列とMIN1列とともに、さらに新規AUTHR列も、送信することができる。この新規AUTHR列はRAND、ESN、MIN1、MIN3およびSSDAの連結のハッシュ処理から得られる(図2には図示せず、というのは第三者にされる呼出がないためである)。いったんこの基地局との対話が設定されてしまうと、実際の情報通信は、所望ならば、SSDBで暗号化され、進むことができる。

【0020】さらにセキュリティを保持するためこの基地局は何時でも再認証を要求できるがこれは前記初期登録と同様に行われる。次にセルラ電話10の保持者に対し顧客クレジットを得る課題に戻る。クレジットを供与しクレジット・センタ40でこのユーザの口座に課金するために必要な最も基本的プロトコルには次のステップが含まれる。

(A) クレジット・センタ40と通信しそれに課金するその口座に関する必要情報とその口座に課金する合計金額を提供するステップと、(B) 業者の機器30によってこの業者にその要求合計金額を帰し債権とすることを通知するステップである。さらにステップを追加して例えば、次項を保証することができれば好都合である。

【0021】それは正しい口座にその提供クレジットを課金することを保証する、さらに正しい業者にその要求合計金額を帰し債権とすることを保証する、さらに侵害者によって現在または将来の損害をこの業者に、またクレジット・センタ40に、またはセルラ電話10のユーザに、加えないことを保証する、などを挙げることができる。その単純な形の一例として、次のステップを持つ詳細プロトコルを示す。

(A) この業者はその顧客に特有のコードを提供するがこれはクレジット・センタ40にこの業者を識別する特有のコードである(図2のライン18)。

【0022】(B) この顧客は次例のような事項をセルラ電話10に加える。例えば、“星印と9”のような接頭部であり、さらにその業者のIDコードであり、さらにこの顧客の口座に課金しその業者に帰し債権とする必要がある合計金額である。これがMIN2列を形成する。

(C) セルラ電話10は、基地局20で先に登録され、またステップ(B)のデータがそのバッファに入力され

ており、その“送信”コマンドに回答してそのMIN2列、RAND列、ESN列、MIN1列およびAUTHR列を送信する、ただしこのAUTHR列はRAND、ESN、MIN1、MIN2およびSSDAの連結のハッシュ処理から得られる(図2のライン14)。

【0023】(D) 基地局がこの送信情報を受信すると、(例えば、その“星印と9”列から)これは通常呼出ではなくクレジット・センタ40に達しようとしているものであることを認める。それに回答してクレジット・センタ40が接触されその関連情報が伝えられる。すなわちこれは、そのESNとMIN1とMIN2のデータである(図2のライン17)。基地局20の認証プロトコルはセルラ電話10が実はその受信したESNとMIN1に対応する電話であることを有効に保証し、したがってクレジット・センタ40はMIN1の顧客がクレジットを得るに値するかその正否を求める位置にある。

【0024】(E) クレジット・センタ40が無線電話10にクレジットを供与する必要があると決定すると、このクレジット・センタは承認コードを業者の機器30に、さらにおそらくそのセルラ電話にも同様に、送信する(図2のライン15、16)。この承認の受信でこの所望のトランザクションは成功裡に終了する。この顧客のクレジット口座に対するこのクレジットの実際の転記記帳は通常のように行われ、またこれは“900サービス”で行われるように、セルラ電話10に対する料金課金レートを変えて行うこともできる。

【0025】以上開示のプロトコルで一つ少し厄介な点はこの業者はそのコードをこの顧客に提供が必要であることで、もしこのステップを音声通信で行うとエラーが生ずることが予想される。さらにまた、クレジット・センタ40が業者の機器と接触する必要があることは少し不都合であり、というのはこれはこの業者のコードを(通常)電話番号に翻訳するデータベースの利用を必要とし、また通信パスを設定するプロセスがさらに時間を取るからである。しかしこれらの欠点は、僅かな変形、例えば、この業者がクレジット・センタ40と、どちらかといえば別の経路で、接触する変形例、またこの業者がその識別コードをそのクレジット・センタに電子的に送信する変形例で克服される。

【0026】当然のことであるが、基地局20を介する無線電話10とクレジット・センタ40間の通信は、業者30とクレジット・センタ40間の通信と(関係しているという意味で)リンクする必要がある。このリンクは、選択したトランザクション・パスワード(TP列)の使用に合意したその業者とこの顧客によって設定することができる。この列データはランダムで過渡的な、例えば、ただ一度だけ使用するような、ものとして行うことができる。この顧客がその業者のIDコードの代わりにこのTP列を入力し、それを基地局20に送信し、その業者が同一TPをクレジット・センタ40との業者の通信

9

に利用することができる。

【0027】このTP列をその業者からこの顧客に音声で通信することができ、この顧客はこのコードをそのセル電話に挿入することができる。これによって近隣のセル電話が誤ってこの通信に加わりそのクレジット金額を負い債務とする危険をなくする。このTP列はただ一度だけ使用されるので侵害者にその価値は無く、このステップでのエラーはそのトランザクションを明白に失敗させるだけに過ぎない。これが生ずる場合には、この顧客とその業者はこのTP列（または異なるTP列）を再入力し再試行することができる。この変形プロトコルによる場合もその電話通信は前の通りであるがここで次の相違点がある。

【0028】それは、この業者の機器はそのクレジット・センタと接触し、身元を明らかにし、このTP列を提供し、適切な場合、そのクレジット・センタから承認または許可を受信する。クレジット・センタ40がこの業者が提供したTP列を無線電話10による通信にリンクするのを助けるため、業者の機器30が無線電話10のESNとMIN1を含むことは好都合である。このプロトコルを図3に示す。当然のことであるが、機器30は無線電話10からそのESNとMIN1の情報を受信する必要があることは機器30に付随する受信機31によって実現することができる。この受信機は低感度受信機とすることができる、というのはその商品やサービスを購入する顧客はこの受信機の近隣にいたことが考えられまたこの業者は隣接するセル電話からの送信を受信しないことを所望する。

【0029】正しいセルラ電話だけの受信を低感度受信機を利用する以外の方法で保証することができる。例えば、機器30の受信機をこのTP列を送信しないセルラ電話からの受信をすべて棄却するようセットすることができる。または機器30が金属シュラウド32をアンテナ31の周囲に有することができ、ただしここに無線電話10のアンテナを挿入するが、これによってその信号のみをアンテナ31が受信するようにする。受信機31が機器30に導入されると、無線電話10と基地局20間の通信が必ず行う必要はなく、またはどうあっても直接行う必要もない。すなわち、機器30は無線電話10の送信を捕え、所望するデータが何であれそれを付加し、この結合情報をクレジット・センタ40へ基地局20を介し（図1のパス22を利用し）送信する。

【0030】または、機器30は基地局20をバイパスして直接そのデータをクレジット・センタ40へ送信することができここではプレプロセッサ42がそのデータを受信し基地局20の登録プロセスをエミュレートする。図4に示すように、業者の機器30はプレプロセッサ42からそのRAND列を得てそれを無線電話10へ送信する。同時にこの業者はそのTP列を無線電話10のユーザへ送信することができる。無線電話10は次の

10

列データを生成する。これには、そのトランザクション・パスワード列（TP）、ESN列、MIN1列があり、またオプションであるがMIN2列があり、さらにAUTHR検証列（このAUTHR列にそのTP列が埋め込まれている）がある。

【0031】次に機器30はこの情報をプレプロセッサ42に送信し、このTP列、その合計金額、そのIDコード、さらにおそらくそのRAND列、を加える。プレプロセッサ42はクレジットを要求するユーザの正当性を確認するがそれは機器30が送信した他のデータに対しこのAUTHR列を解析して行い、そしてクレジットを供与するかその正否を決定する。次にこの判断は機器30へ、さらにオプションであるが無線電話10へ、送信される。この顧客の口座に課金する金額の書面での確認はこの業者がその顧客にプリントアウトを提供し行うことができ、また所望に応じこのプリントアウトにこの顧客が署名しこの課金のバックアップ検証とすることができる。このプリンタは図1では装置33で示す。

【0032】図1に示すシステムに必要なハードウェアについてはその機器は全く通常の機器である。例えば、セルラ電話10も通常のセルラ電話であり、また基地局20、50も同様に通常の基地局である。この業者の機器は単に基地局20の受信機に類似のまたはさらに簡単な受信機であって、実施する必要があることはただ信号の受信で正しい入力信号を優先するよう受信信号を判別することだけである。この場合購入を所望する顧客のセルラ電話はその業者の受信機に対し最も近接した次のセルラ電話に比べ少くとも2倍接近していることが期待される。シュラウド32はこのような判別にエラーを小さくする有効なものである。

【0033】そこで入力する電力に基く判別は簡単で有効である。しかしまたこのような判別はそのTP列がセルラ電話10からの通信に含まれていることを単に確認するだけで実施可能であることを思い出すことができる。このことからAUTHRに埋め込みかつ“遮るものの無い自由空間”にこのTP列をそのセルラ電話が出力する必要がある。業者の機器30にはこの受信機に加えてその受信データに情報を追加しこのデータをクレジット・センタ40に送信する手段が必要である。このような機器は通常のPCでまたは特定のハードウェア配置でただし多機能の点でも価格の点でも低いもので、これ容易に実現することができる。

【0034】ここでプリンタには通常のクレジット・カードに関しては現在普通に使用されているプリンタのいずれの種類でも利用することができる。クレジット・センタ40に関しては、これはほとんどの場合通信とデータベースの中心役割となるオフィスであって現在のセルラ電話提供者のビジネス・オフィスとそう変わらないものである。

【0035】2. ホーム帰還

11

前記私的に出掛ける例のようなショッピングの後、セルラ電話の保持者はそのホームへのアクセスを所望し同じセルラ電話の制御下でガレージ・ドアの開錠を所望する。この目的のためにはクレジット・センタ40に係る必要はない、というのはここではクレジットが供与されることはない（ただし、例えば、その基地局によってこの制御トランザクションが行われその寄与に対して負う課金の場合は当然除外する）。以上概要を述べたタスクは単に一つのガレージ・ドア開錠機の制御例であって必要条件ではないが下記のようにさらに通信が含まれる例もある。通信の実施の形態例では、ガレージ・ドア開錠機はセルラ電話受信機で読取手段が追加されたものである。

【0036】次に動作で説明する。このガレージ・ドア開錠機をそのセルラ電話基地局で登録し、この基地局がそのSSDA列とSSDB列をそこに組込むことができる。要点は、この基地局は保証された仕方でのそのガレージ・ドア開錠機と通信し、これは他のセルラ電話の場合とほとんど同様であるが、相違点はこの基地局からガレージ・ドア受信機への一方向通信のみということである。このセルラ電話10がそのガレージ・ドアを開錠させたいと所望する場合、その基地局にこのガレージ・ドア受信機に呼出を行わせコマンド列データをその受信機に送信するように要求する。このデータ列に含むものに次のものがある。

【0037】それには、乱数(RANDX)があってこれはこのセルラ電話の保持者によって“打込まれ”たもの(そのTP列、トランザクション・パスワードで、このトランザクションに対するもの)であり、さらにセルラ電話10に蓄積したキー(B-KEY)でこの乱数をハッシュ処理したものである。前述のように、この受信機には読取手段があってこれはそのB-KEYでハッシュ処理した列データを回収する読取手段である。この読取乱数が“遮るものの無い自由空間”で受信した乱数に対応する場合、そのガレージ・ドアは開錠される。このプロトコルを図5に示し、ここでライン11、12、13が、図2について述べたように、その登録プロセスを示す。

【0038】ここでこのセルラ電話は、通常の電話結合のプロトコルからは図5で少し異なるプロトコルに従うことが分かる。具体的には、この被呼側電話番号(MIN3)を単に送信しその基地局からこの被呼者が応答した表示を待つ代わりに、そのRANDX列とB-KEY(RANDX)列を直ちに追加する。これは、このセルラ電話が容易に認識できる(およびさもないければ有効な列データに対応しない)シーケンス、例えば、“8”、ただしさらにユーザが供給するRANDX列が続くが、これをこのセルラ電話では選択することによって容易に行われる。または、セルラ電話10は、考えられることであるが、このMIN3信号を送信し、クリアツーセン

12

ド信号を待ち、次にそのシーケンスの残部を送信する。

【0039】通信を含まない実施の形態例では、このセルラ電話基地局はなお次のような意味を持って動作する。つまり、このセルラ電話はその基地局と自動的に対話しこのセルラ電話の電源を入れると直ちに自ら届出て登録する。換言すると、好むと好まざるとにかかわらず、このセルラ電話の電源を入れると、その基地局に自ら届出て登録する。この活動は、通常、そのセルラ電話保持者のクレジット口座に課金を生成しない。この登録点以上には通信を含まない実施の形態例ではその基地局からの手助け無しにこのガレージ・ドアを開錠することが本目的である。

【0040】これは多数の方法で達成されるが次の点が必要である。それは、(図5の)ライン13の“OK”信号に続くこの基地局へ送信される信号はこの基地局には分からないものであることが必要である。逆に、このガレージ・ドア受信機はそのセルラ電話からのその送信に同調しその送信が分かる必要がある。これは次例のように達成することができる。例えば、このガレージ・ドア受信機がその基地局の“OK”信号、ただしこれはこのセルラ電話に特定の周波数で動作するよう指示する信号であるが、この送信を傍受して実現できる。次にこの受信機はその同じ周波数に自ら同調してこのセルラ電話の送信を捕えることができる。

【0041】図6に示すように、次にセルラ電話10が図5のライン25の信号を送信すると、この受信機はそれを傍受し、それを読取し、そこでそのガレージ・ドアが応答する。このような実施の形態例では、MIN3はその基地局が認識しない列データであって、またはAUTHRを削除するかまたは単に変更してその基地局によって拒否を起こさせる。または、その“8”シーケンスをセルラ電話10に挿入すると、登録用に用いる固定呼掛け周波数に自ら同調することができる。このような実現に、このガレージ・ドア開錠機はその呼掛け周波数に固定的に同調することができる。ここでガレージ・ドア開錠の前記例は一例であって他の制御利用、例えば、自動車ドアや家の開錠、アラーム起動を挙げることができ、これらも本発明の技術的範囲に包含される。

【0042】3. 制御拡張

そのホームへ所望通りアクセスできると、セルラ電話10の保持者は種々の機器の制御を所望することができる。このような利用の場合にはセキュリティは、前記2例の利用の場合のような関心のあることではない。さらにまた公共ポリシーの観点からもこの基地局をこのような制御利用には含まないことが望ましい。後者の場合はこの基地局によってカバーされない帯域にこのセルラ電話の動作周波数を単に変更するだけで実施可能である。次に動作で説明する。各ホームにはそれ自身のホーム・コントローラ基地局があってこれが選択された周波数で動作する。スイッチまたは“打込んだ”コードによって

13

このセルラ電話を“ホーム・コントローラ”モードにすることができ、このモードではこのセルラ電話はそのホーム・コントローラ基地局とだけ対話する。

【0043】次にこのホーム・コントローラ基地局は通常の方法を用いてそれにいかなる制御が割り当てられてもそれを実行することができる。この認証プロセスは前記のように行うことができるが、ただしこのホーム・コントローラ基地局の制御下に行われる。すなわち、このホーム・コントローラ基地局は、その所望のインタラクションに基づきホーム・コントローラとしてそのセルラ電話を認証する機能を含むことができ、ただしそれに限る必要はなく、または選択的にそれをすることもできる。例えば、ホーム・コントローラとしてこのセルラ電話を利用してTVチャンネルを変えることができ、そのためにおそらくあるセキュリティ処理を所望することも可能である。

【0044】しかしまたこのセルラ電話を利用してそのテレビジョン信号供給元と対話することもできるがただしここではセキュリティを求めなくてよい。このようなインタラクションによって購入を行うことも可能であってホーム・コントローラのオーナーは訪問者にこのホーム・コントローラ基地局をコンジットとして利用させても気にしなくても差支えない。以上開示の配置を図7に示し、ここにはホーム基地局60があり、さらに種々のホーム・コントローラ61があってこれが機器を制御し、この機器には例えば、テレビジョン“セット・トップ・ボックス”62があり、またテレビジョン63があり、さらにこのテレビジョン上に広告された商品および／またはサービスの供給元と対話できる手段64がある。

【0045】このような手段をそのセット・トップ・ボックスの一部とすることも可能であってこれはそのテレビジョン信号の供給元（図示するが）へ信号を返送するが、またそれに限る必要もない。ここで付記すべきことは本発明の以上の説明はセルラ電話に限るものではない。いずれの種類の無線手段でも以上開示の機能を実現することができるが、ただしそれはこのような手段が手元の利用に対し適当な認証能力を持つ場合であって、しかし以上説明のように所望の認証機能が重要でなくまたは全く不要であるような利用の場合もある。以上の説明は、本発明の実施の一形態例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例が考え得るが、それらはいずれも本発明の技術的範囲に包含される。尚、特許請求の範囲に記載した参照番号は発明の容

14

易なる理解のために、その技術的範囲を制限するよう解釈されるべきではない。

【0046】

【発明の効果】以上述べたごとく、本発明によって、認証したトランザクション・コントローラで、例えば、セルラ電話を利用して顧客クレジットで金額交換を行い、またホーム・ガレージ・ドアを開錠させ、さらにテレビジョン広告の商品やサービスの対話に利用でき、有効な認証したトランザクション・コントローラを提供することができ、通信利用にさらに多機能利用を加えた高度利用の有用な無線電話システムを提供することができる。

【図面の簡単な説明】

【図1】本発明のシステムを実行する配置を示す図である。

【図2】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図3】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図4】本発明のシステムに使用するプロトコル例のフローを示す流れ図である。

【図5】保証制御利用のためのフローを示す流れ図である。

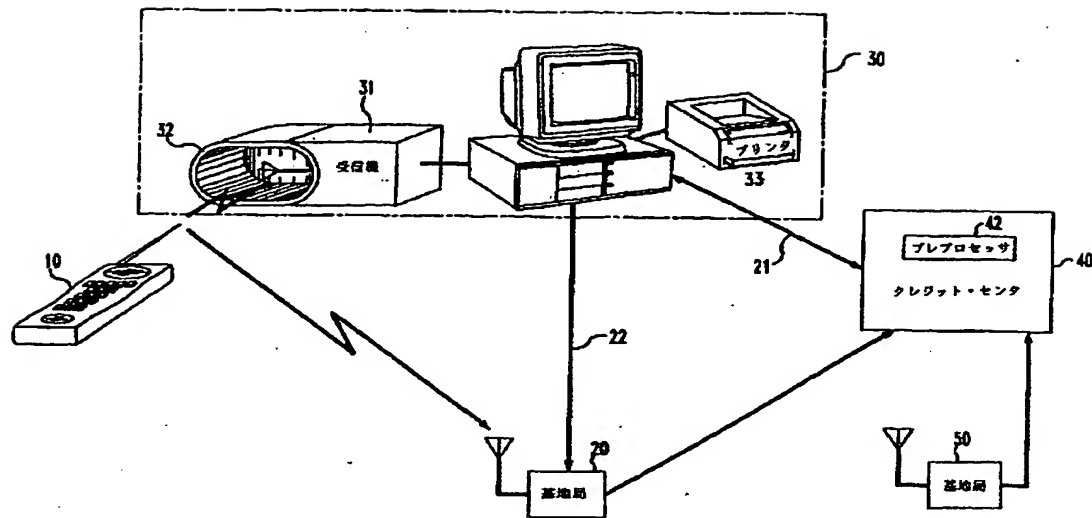
【図6】保証制御利用のためのフローを示す流れ図である。

【図7】ホーム・コントローラ基地局配置を示す図である。

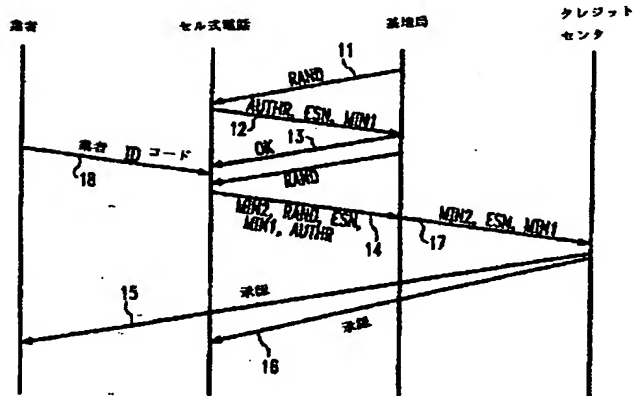
【符号の説明】

- 10 セルラ電話
- 20 無線電話基地局
- 21 チャンネル
- 22 バス
- 30 (販売業者) 機器
- 31 受信装置
- 32 シュラウド
- 33 プリンタ
- 40 クレジット・センタ
- 42 プレプロセッサ
- 50 無線電話基地局
- 60 ホーム・コントローラ基地局
- 61 ホーム・コントローラ
- 62 セット・トップ・ボックス
- 63 テレビジョン
- 64 コントローラ

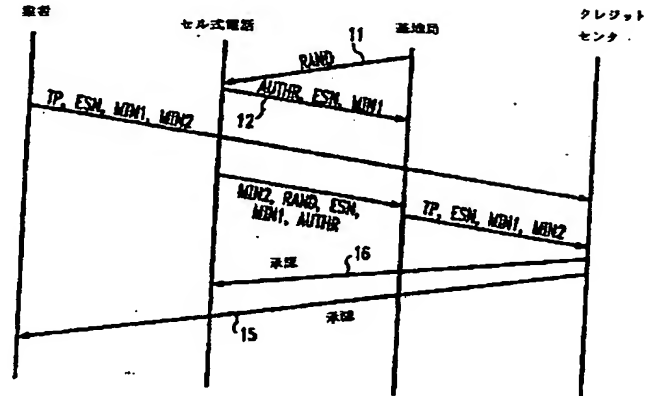
【図 1】



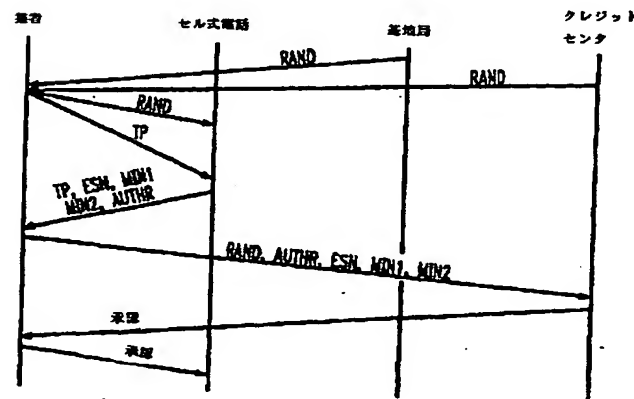
【図 2】



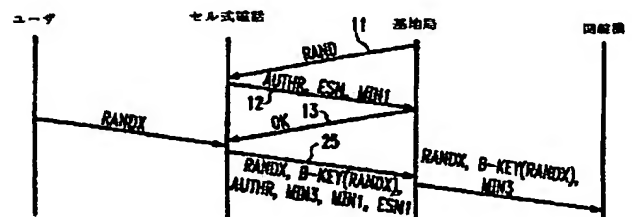
【図 3】



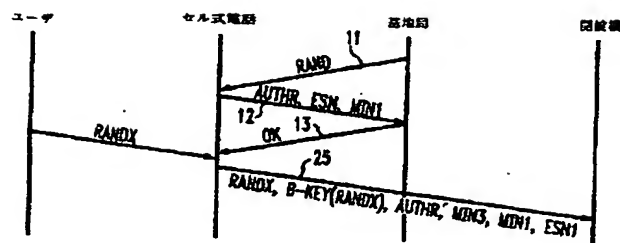
【図 4】



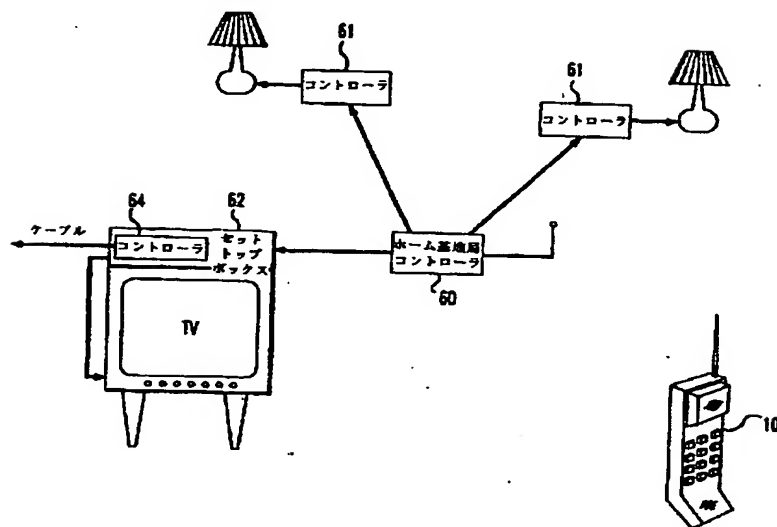
【図 5】



【図 6】



【図 7】



フロントページの続き

(51) Int. Cl.⁶

識別記号

庁内整理番号

F I

H 0 4 B 7/26

技術表示箇所

1 0 9 S

1 0 9 J